디지털 콘텐츠 보호를 위한

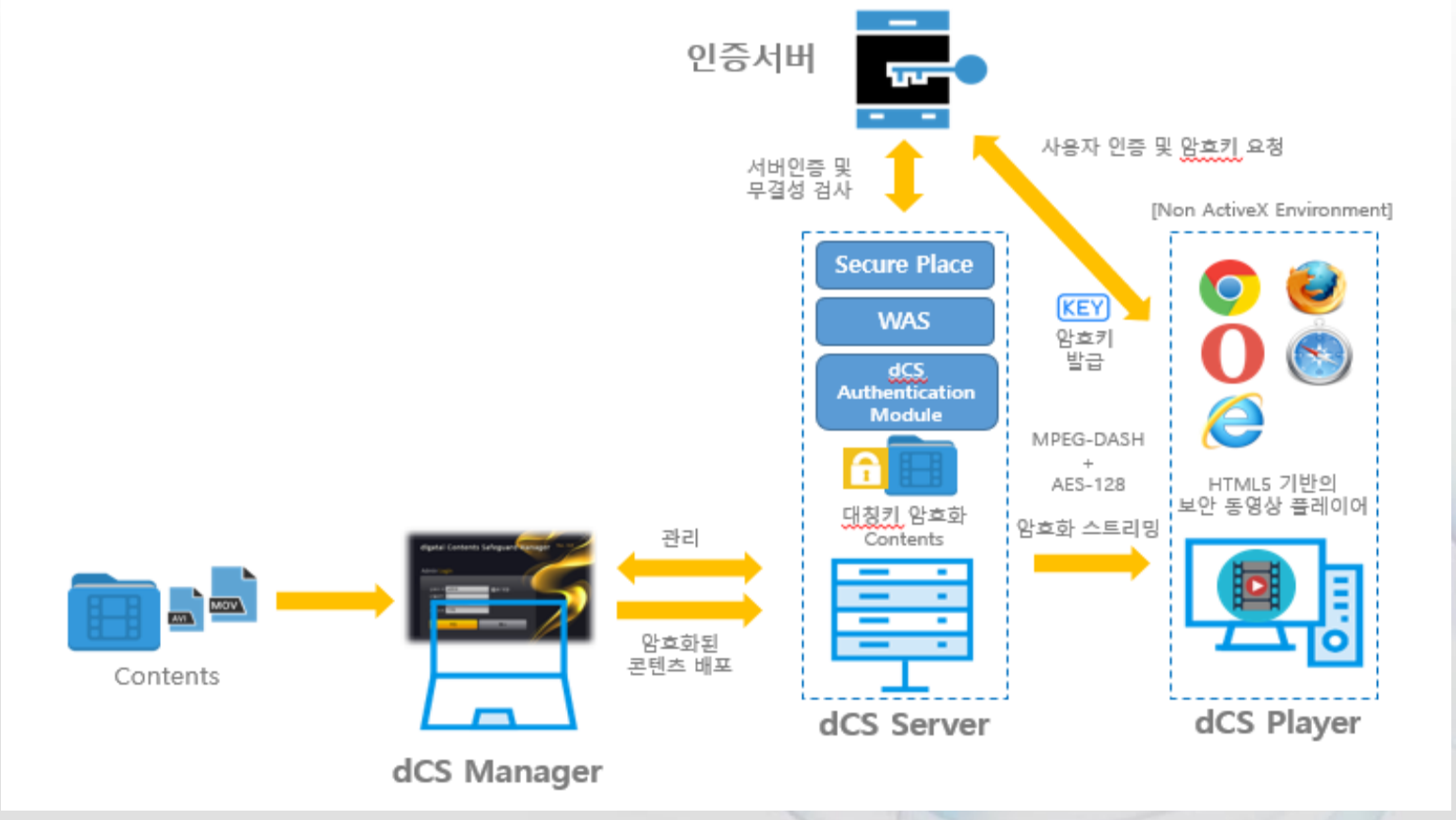
dCS(digital Contents Safeguard) 소개서

목차

1. dCS 개요

dCS(Digital Contents Safeguard)개요

- 동영상 콘텐츠의 불법 복제 및 유출을 방지하고, 유통과정에서 투명성과 신뢰성을 보장하여 공급 및 유통, 서비스까지의 모든 과정을 보호하는 솔루션



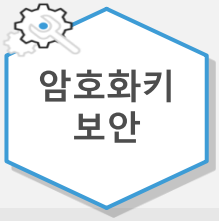
2. Why dCS?

dCS 도입 필요성

필요성 01 •• 서버 내 콘텐츠 유출의 위험

- 내부 임직원, 협력업체 등에 의한 서버 내 콘텐츠 유출의 위험
- 해킹에 의한 콘텐츠 유출의 위험

필요성 02 •• 서버 내 단일 암호화키 방식의 보안 위협



- 기존 솔루션의 경우, 단일 암호화키 방식으로 인한 보안 취약성 존재

필요성 03 •• 다양한 사용자 환경의 지원 필요

- 기존 DRM의 경우, 다양한 사용자 환경을 지원하지 못함
- 사용자 편의성을 제공하지 못하는 경우, 비즈니스 한계에 봉착함

3. dCS 특장점

HTML5 기반 동영상 플레이어

1. 실시간 암호화 처리

- AES-128 동적 암호화된 스트리밍 동영상을 실시간 처리
- HTTPS(TLS) 적용으로 안전한 통신 서비스 제공

2. 사용자 편의성

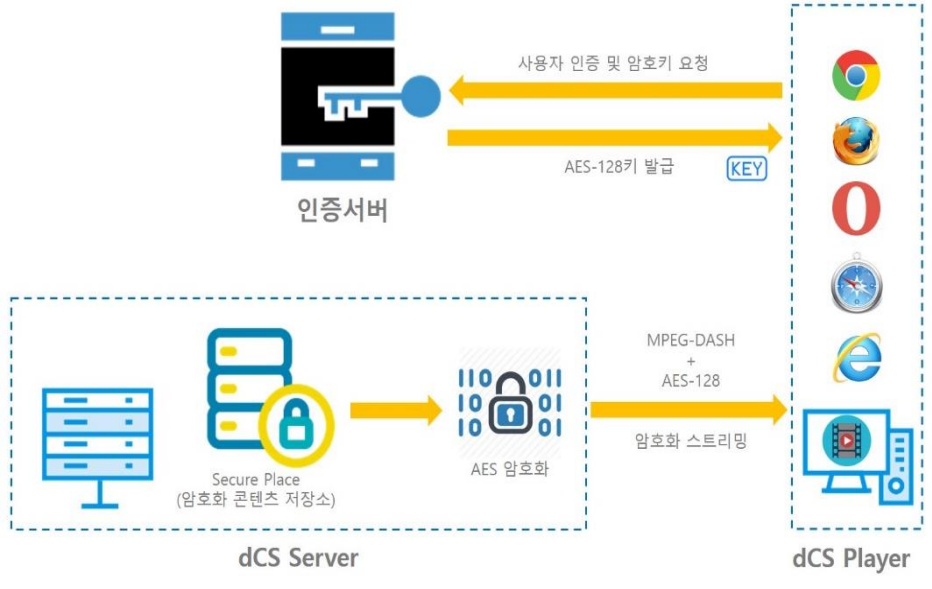
- 특정 브라우저의 종속성 없이 서비스 가능(Non-ActiveX 환경)
- PC, Tablet, Mobile 등 다양한 기기에 스트리밍 서비스 지원

3. 비용 절감

- 별도의 미디어서버 없이 웹서버만으로 스트리밍 서비스 제공
- 환경변화에 따른 플레이어 업그레이드 및 이슈 발생하지 않음

3. dCS 특장점

OPEN TEE 기반의 안전한 인증키 관리



1. 인증서버 분리

- 인증키 분리관리로 인한 보안 강화
- 원격의 콘텐츠 서버 인증 지원

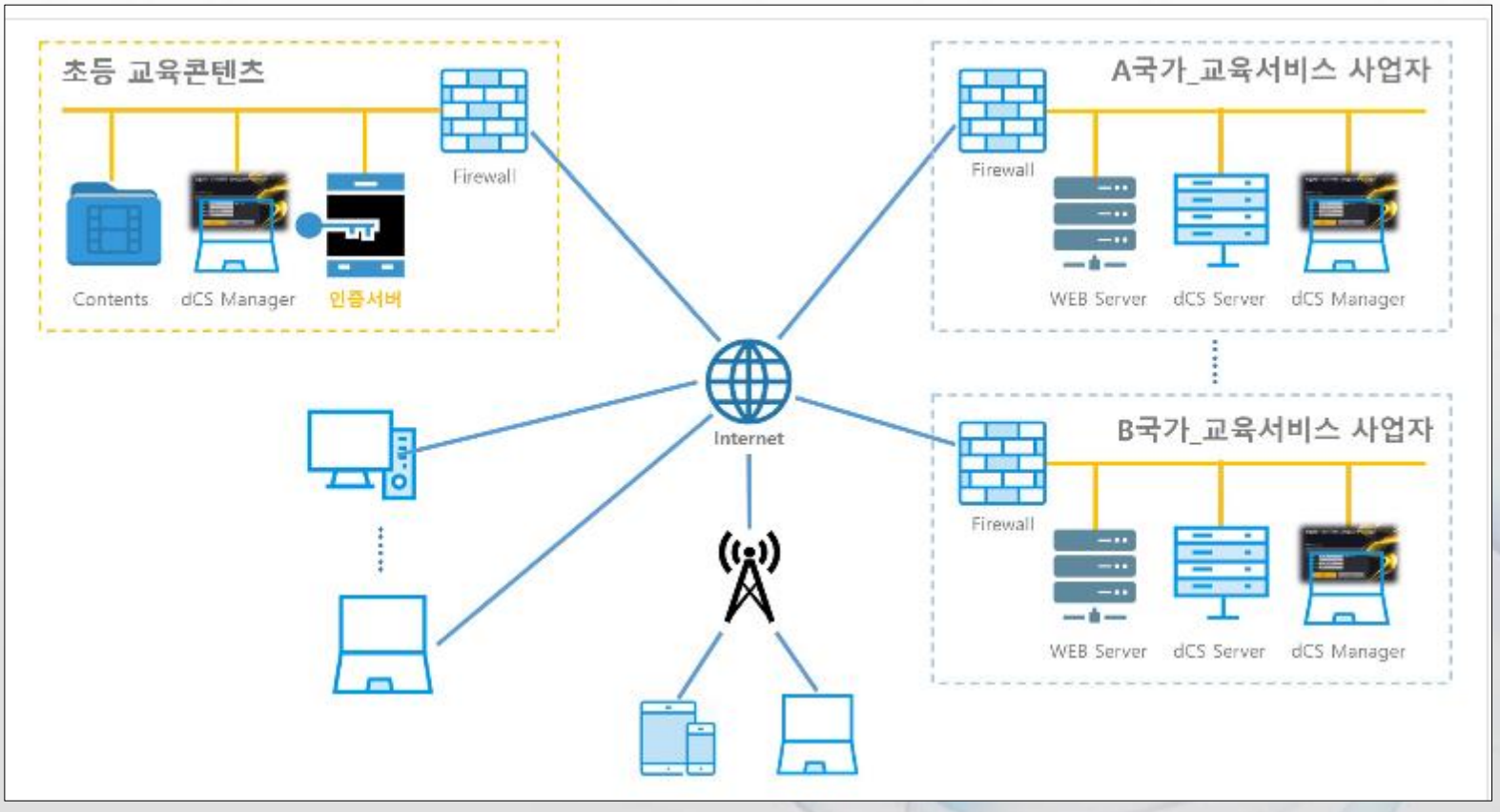
2. Open TEE 기반 콘텐츠 암호화

- Open TEE 기반의 콘텐츠 암,복호화 수행
- 암호화키는 Secure Place에 안전하게 보관

3. dCS 특장점

다양한 비즈니스 모델 지원

- 다양한 서비스 모델 제공(B2C, B2B 등)
- 별도의 미디어 서버 없이 웹서버만으로 스트리밍 서비스 가능
- 사용료 지불을 위한 과금 시스템 연동 가능



4. 주요기능

Secure Place & Trusted Execution

1. Secure Place

- 콘텐츠 암호화키를 보안영역에 보관하여 기밀성 유지
- 랜덤함수를 이용한 암호화키 생성
- Open-SSL 및 AES-128 알고리즘 적용으로 암호화 성능 최적화

2. Trusted Execution

- 암 · 복호화 및 인증과 관련된 모든 함수 처리

4. 주요기능

Server 간 상호인증

1. 상호인증을 통한 인증강화

- 인증서버와 웹 서버 상호인증을 통한 인증강화
- 콘텐츠 유출 방지
- 콘텐츠 임의 변경 방지(무결성 강화)

2. 전송구간 Open-SSL적용

4. 주요기능

콘텐츠 암,복호화

1. 콘텐츠 암호화

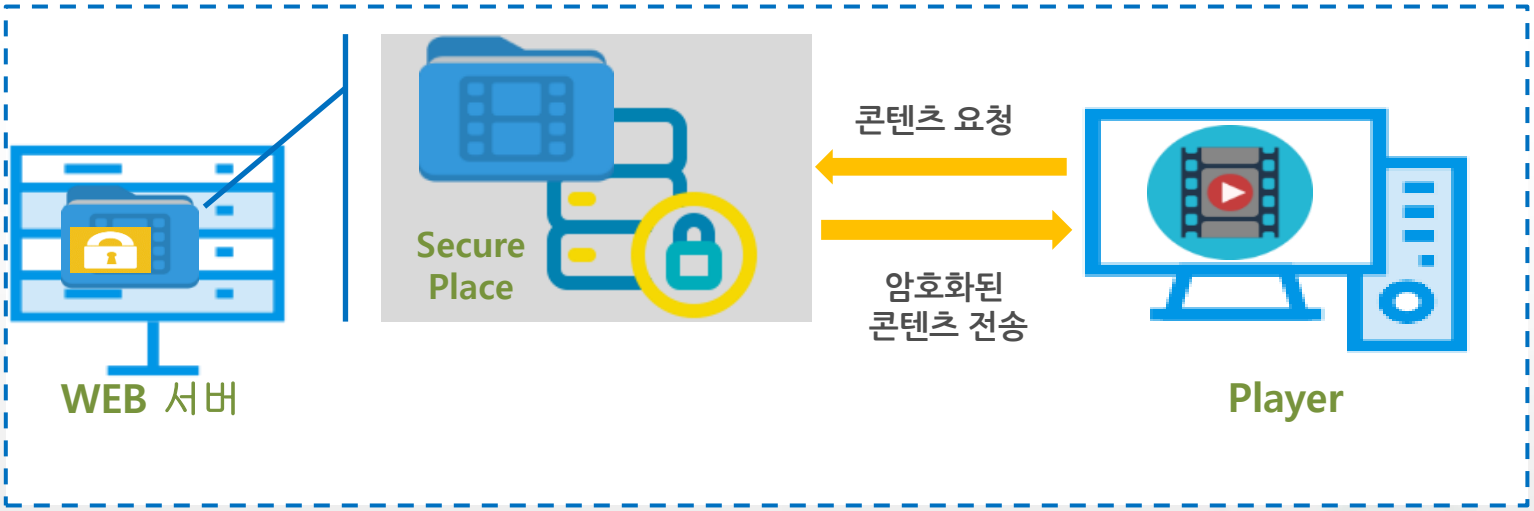
- dCS 서버에 콘텐츠를 OpenTEE 기반의 암호화로 관리
- 콘텐츠 암호화키는 dCS서버내 Secure Place에 저장

2. 콘텐츠 복호화

- dCS 서버내 콘텐츠를 OpenTEE 기반의 복호화 진행 후 전송
- 전송시, 인증서버에서 수신한 AES-128키로 암호화하여 전송
- dCS Player에서는 인증서버에서 수신한 AES-128키로 복호화

4. 주요기능

콘텐츠 전송

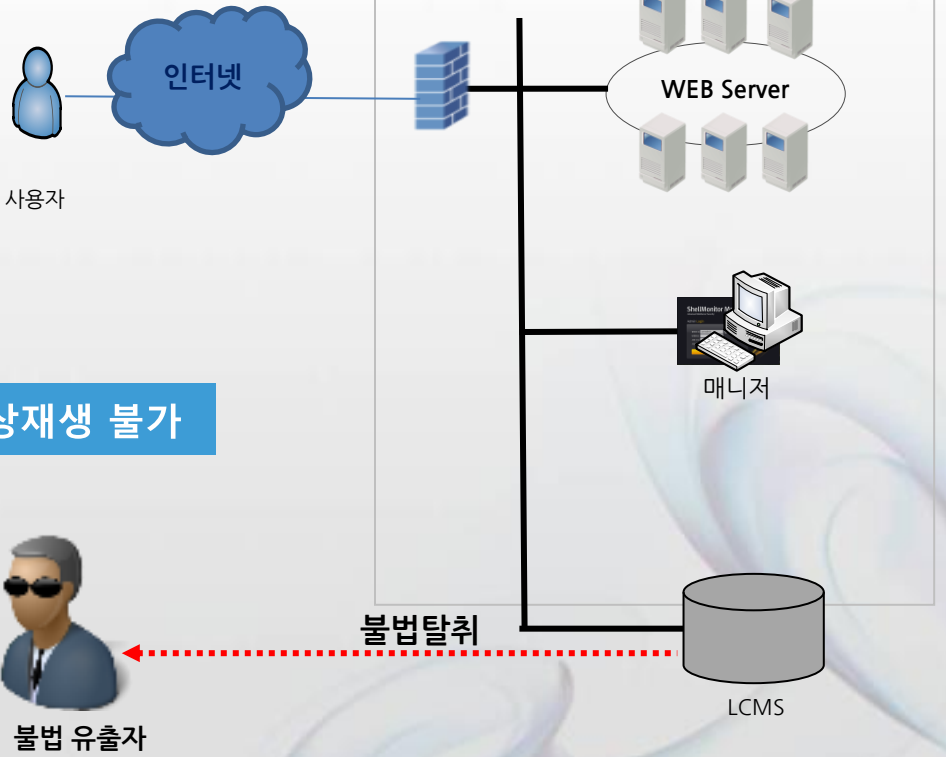


실시간 암,복호화

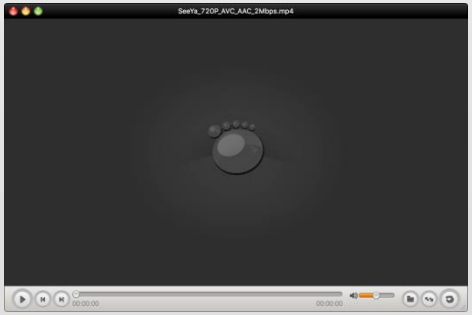
- 암호화된 콘텐츠가 인증을 거친 후 암호화된 콘텐츠로 전송
- 사용자 Player에서 복호화 하면서 실시간 시청
- 전송구간 Open-SSL 적용

적용 예시

사용자 인증 후 영상 재생가능



비정상적인 자료 접근 시, 영상재생 불가



5. 활용 방안

기대효과

기대효과 01 • • 콘텐츠 보호

콘텐츠 보호

- 관리자 및 해킹에 의한 콘텐츠 임의 변경 및 유출 방지
- 운영을 위한 핵심 데이터는 Secure Place에서 안전하게 관리
- 파일 단위의 콘텐츠 암호화 모듈 제공

기대효과 02 • • 서비스 운용 및 관리

서비스 운용 및 관리

- 상호 인증을 통한 실시간 웹서버 이상 상태 확인
- 최적의 암,복호화 기법 사용하여 원본 콘텐츠 속도와 동일한 수준의 속도 보장

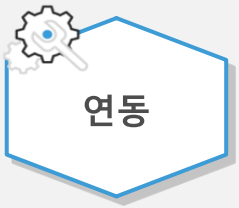
5. 활용 방안

연동방안

활용방안 01 •• CMS 콘텐츠 암호화

- 콘텐츠 암호 및 인증키 관리 모듈 제공

활용방안 02 •• 기존 서비스 관리 프로그램 연동내역



- API를 통한 연동
- 연동내역
  - 인증실패, 통신실패, 서버정보(서버이름, 도메인 이름, 서버 IP정보)

활용방안 03 •• 콘텐츠 복호화 지원

- 암호화된 콘텐츠 Play를 위한 복호화 API 제공
- Open / Play / Seek / Close 기능

5. 활용 방안

추가 웹 서비스 보호 방안 – WSS 연동

콘텐츠 서비스 서버 보호

- WSS(Web Server Safeguard) 솔루션과 연동
- 웹 소스 검사 : 웹쉘, 악성 URL 탐지 및 검열
- 웹 APT 공격 탐지 : 소스코드, 데이터, 환경설정 파일 임의 변경 탐지
- 웹 APT 공격 방어 : 내부 또는 외부 취약점 공격 대응 및 자동 방어 지원

이용자 PC 보호

- 악성 URL은 웹서버를 악성코드의 경유지로 이용하여 바이러스, 랜섬웨어 등을 PC에 대량으로 유포하는 URL 또는 IP주소로 콘텐츠 서비스 서버에 악성 URL이 삽입될 경우 서비스 이용자 PC가 해킹에 노출
- WSS는 Black list & White list 방법을 통해 악성 URL을 실시간 탐지 및 제거하여 콘텐츠 서비스를 이용하는 사용자 PC를 해킹 공격으로부터 보호

5. 활용 방안

사업 제휴

신뢰 시장확대 새로운 서비스

Contents
Service
Platform
PC/Tablet/Smart
Phone

+

dCS
WSS
Web/WAS Server
umv 웹서버·클라우드 컴퓨팅 보안기업 (주)유엠브이기술

Contents Service Platform

감사합니다!